IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISON

UNITED STATES OF AMERICA Plaintiff, v. FLOYD O'HARA Defendant.	))))))))	Case Number: 16 CR 734

MOTION AND MEMORANDUM OF LAW IN SUPPORT OF MR. O'HARA'S REQUEST FOR A *FRANKS* HEARING

NOW COMES the Defendant, Floyd O'Hara ("Mr. O'Hara"), by and through his attorneys, Gal Pissetzky and Adam Bolotin, and respectfully requests that this Honorable Court grant Mr. O'Hara's request for an evidentiary hearing in accordance with *Franks v. Delaware*, 438 U.S. 154 (1978). In support of this motion, Mr. O'Hara files this motion and memorandum of law in support thereof, and states the following:

BACKGROUND

According to the Affidavit for Search Warrant, between January 21, 2016 and January 27, 2016, Detective Richard Wistocki ("Detective Wistocki") of the Naperville Police Department used the "ICAC COPS website and its associated software tools" to observe IP address 173.15.56.62 (EPA IP address) "seeking and attempting to download hundreds of files containing child pornography through BitTorrent." Exhibit 1 - Search Warrant Aff. 12-13 (hereinafter S.W. Aff.). Detective Wistocki "cross-referenced the downloads through the ICAC COPS web site database and confirmed that a computer assigned to the [EPA IP address] was seeking known child pornography files listed in the ICAC database." *Id.* The Affidavit claimed that specific IP address "was the sole candidate for each download." *Id.*

Detective Wistocki then compared the "specific hash values" he observed and compared them to "the hash values in Detective Wistocki's image library of child pornography." *Id.* Wistocki further claimed that "upon comparing the hash values and images that the computer assigned to the [EPA IP address] was downloading with the same hash values and images in the ICAC data base image library, Detective Wistocki confirmed that [the EPA IP address's] hash values were indeed child pornographic images." *Id.* The Affidavit then describes "four of those downloads" that Detective Wistocki observed. *Id.* at 13-14. Specifically, Detective Wistocki asserted that Download 1 was an image of child pornography that the EPA IP address downloaded on January 27, 2016 at 6:02 a.m.; Download 2 was an image of child pornography that the EPA IP address downloaded on January 27, 2016 at 6:02 a.m.; Download 3 was a video depicting child pornography that the EPA IP address downloaded on January 26, 2016 at 5:31 a.m.; and Download 4 was a video depicting child pornography that the EPA IP address downloaded on January 26, 2016 at 5:31 a.m. *Id.* at 13-14.

The Affidavit then details how law enforcement determined that the IP address in question was assigned to the Environmental Protection Agency offices in Chicago, and that nine EPA Information Technology employees had knowledge of and access to that IP address. *Id.* at 15-17. Law enforcement then obtained those nine employees' home IP addresses. *Id.* at 17. Detective Wistocki used the ICAC COPS website and "determined that a computer assigned to the IP address 50.4.103.68 (one of those employees' IP addresses, hereinafter Mr. O'Hara's IP address) . . . had downloaded hundreds of files of child pornography through BitTorrent." *Id.* at 18. Detective Wistocki asserted that "many of the BitTorrent infohashes sought by [Mr. O'Hara's IP address] were identical to the infohashes downloaded through the [EPA IP address] . . . meaning they had the same series of photos or videos, most of which were child pornography." *Id.*

Based on the Affidavit's claims, U.S. Magistrate Judge Sheila Finnegan found there was probable cause and issued a search warrant that granted law enforcement authority to search Mr. O'Hara's home and EPA offices associated with his employment. During the search, law enforcement seized evidence the government intends to use to prosecute Mr. O'Hara.

ARGUMENT

I. Mr. O'Hara is Entitled to a *Franks* Hearing Because Judge Finnegan's Finding of Probable Cause was Based on Material False Statements

A. Legal Standard

The Fourth Amendment provides "the right of the people to be secured in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated." U.S. Const. amend. IV. The Fourth Amendment further shields citizens from law enforcement action, commanding that "no warrants shall issue but upon probable cause, supported by Oath or affirmation." *Id.* A Warrantless search of a home is presumptively unreasonable. *Payton*, 445 U.S. at 586. Thus, absent any exigent circumstances to enter and search a home, the Fourth Amendment's warrant requirement mandates that "the police must obtain a warrant from a neutral magistrate before searching private property." *United States v. McMurtrey*, 704 F.3d 502, 508 (7th Cir. 2013). The affidavit supporting the request for the warrant "must provide the magistrate with a substantial basis for determining the existence of probable cause." *Illinois v. Gates*, 462 U.S. 213, 239 (1983). Probable cause must be founded upon a truthful, factual showing. *Franks v. Delaware*, 438 U.S. 154, 155 (1978).

In *Franks*, the Supreme Court held that intentionally or recklessly submitting false statements in an affidavit submitted in support of a search warrant violates the Fourth Amendment. *Franks*, 438 U.S. 154. *Franks* further held that the Fourth Amendment permits the accused to request a hearing to determine the veracity of the warrant. *Id.* at 155-56. To obtain a *Franks*

hearing, the accused must make a preliminary showing that "(1) the affidavit in support of the warrant contains false statements or misleading omissions, (2) the false statements or omissions were made deliberately or with reckless disregard for the truth, and (3) probable cause would not have existed without the false statements and/or omissions." *United States v. Williams*, 718 F.3d 644, 649 (7th Cir. 2013). The accused must identify specific portions of the warrant affidavit as intentional or reckless misrepresentations, and substantiate the claims by sworn statements. *Franks*, 438 U.S. at 171.

B. The Affidavit Contains False Statements

The Affidavit in support of the search warrant details what Detective Wistocki purportedly did and discovered during the course of his investigation. As described above, Detective Wistocki claims he observed the EPA IP address "seeking and attempting to *download* hundreds of *files* containing child pornography through BitTorrent," and that he "observed these *transactions* by using the ICAC COPS website and *its associated software tools*." S.W. Aff. 13. These bold claims are the first of many material false statements contained in the Affidavit.

It is important to clarify how users obtain files through BitTorrent client software, what certain tech terms mean, and what certain law enforcement software tools enable officers to discover. Beginning first with BitTorrent client software. In order to obtain a file, a user first downloads a BitTorrent client software program. Next, the user searches for torrents within their BitTorrent client. Here, Mr. O'Hara used Tribler as his BiTorrent client software. This search will generate a list of torrents. A "torrent" is a text file proprietary to the BitTorrent network that contains instructions for torrent client software on how to download a file or sets of files on the BitTorrent network. Torrent files do not contain data such as images or videos, but rather an index containing information about the files associated with that torrent including but not limited to,

names of the files instructed to download, the torrent author, the date the author of the torrent created the file, the number of files the torrent is set to download, and the URLs tracking the torrent activity. A user will not have the actual files until the torrent is parsed or seeded. In this regard, users may have torrents without ever having the associated viewable files. Also, not every file described by the torrent is related or responsive to the search term entered by the user. If the torrent comes up in the search, it does not mean that every file described by the torrent is relevant to the search term. It only means the torrent describes at least one file responsive to the search.

It cannot be stressed enough that neither info hashes, the torrents they reference, the file names or hashes values contained within the torrent are synonymous with downloaded files or attempts to download a file. Again, a torrent is a "catalog" that does not contain any content whatsoever. A torrent only provides information about files available on the BitTorrent network. By possessing a torrent, the user contains information about files on the BitTorrent network (not even necessarily searched for) and may be unknowingly/unwillingly advertising that information on the network without actually possessing the files detailed in the torrent

Downloading a specific torrent does not mean that a user has ever downloaded, or is in the process of downloading any particular file described within the torrent. As the search warrant affidavit correctly detailed, after accessing the torrent, "a user can download some or all of the files associated with the torrent." S.W. Aff. 8. The user can also choose to not download any of the files associated with the torrent. After the user downloads the torrent, if he wants a file, he must load the torrent into the BitTorrent program. The BitTorrent program will then download the file originally searched for, as well as potentially other files not search for. A user will not obtain an actual image or video file detailed within the torrent, unless a user specifically downloads the image or video file and it has been parsed by BiTorrent software.

A problematic aspect of this process is what the software program does when a user uploads the torrent into the program. When the user uploads the torrent, the Tribler software program creates a hidden system file labeled tribler.sdb. The .sdb file stores every file name, hash value, and other descriptive information contained within the torrent. This is especially problematic because the Tribler program will broadcast that the user is now associated with every file listed in the torrent when in reality he only searched for a single file.

The entire process can be described as this example. After downloading the BitTorrent software program Tribler, a user searches for a book. The user may then download a torrent if he someday wants to download the book file. The torrent contains information that describes that book file, and countless other files that the user did not search for. The user is not even able to see what other files the torrent describes. Simply accessing the torrent does not, however, give him the book. Instead, at this point he would only obtain the torrent that contains the book file's and those countless other unknown files' names, hash values, and other information. The user does not possess that book unless and until, after accessing the torrent, he uploads it to his BitTorrent software program. Though the user does not download or begin to download any of the torrent's described files until he uploads it to the software program. By uploading the torrent, the software program will only download the book file he originally searched for. Unbeknownst to the user, the program will also create the hidden tribler.sdb database file that details every file name, and info hash value of torrents. This hidden database file will falsely advertise that the user is associated with torrents even if no files have ever been downloaded, despite the user only downloading one single pdf book file.

Turning to law enforcement software. ICAC COPS is simply a database that lists info hashes, *i.e.* torrents, that other individual officers believe might contain descriptions of files of

interest. The ICAC COPS database also provides file names and hash values that officers believe belong to files of interest. The ICAC COPS database does not enable officers to see what specific file a particular IP address has downloaded, or is in the process of downloading. The ICAC COPS database does not enable law enforcement to discover what search terms a user entered that led him to a specific torrent. Torrential Downpour is another software tool utilized by law enforcement that searches for info hashes values that have been deemed to be associated with files of interest. Torrential Downpour will generate a report that lists IP address that are deemed to have associated with certain info hashes values of torrents. Torrential Downpour does not enable law enforcement to learn what search terms a user entered that led him to a specific torrent, or what, if any, files the user actually possesses from that torrent – unless a single source download is conducted.

All of these facts stand in direct contrast with what the Affidavit represents. Detective Wistocki could not possibly have used ICAC COPS to observe the EPA IP address "seeking and attempting to download hundreds of files of child pornography." As described above, ICAC COPS does not enable law enforcement to see specific files that an IP address is searching for, in the process of downloading, or has fully downloaded. In reality, Detective Wistocki implemented Torrential Downpour which generated a report that detailed that the EPA IP address was associated with a certain info hashes, *i.e.* torrents. This is not synonymous with seeing searches or downloads. As described above, accessing a torrent only gives users names of files. In no uncertain terms, the Affidavit flat out lied when it represented that Detective Wistocki observed the EPA IP address seeking and attempting to download hundreds of files containing child pornography.

The Affidavit then asserts that "Detective Wistocki cross-reference the *downloads* through the ICAC COPS web site database." S.W. Aff. 13 (emphasis added). Specifically, Detective Wistocki claims he "compared the hash values and *images* that the [EPA IP address] was

downloading with the same hash values and images in the ICAC database image library." *Id.* (emphasis added). According to Detective Wistocki, this cross-referencing allowed him to confirm that the hash values he observed were child pornographic images. *Id.* This is just lies on top of lies. In reality, Detective Wistocki did not see any downloads or images, but only observed the EPA IP address to be associated with a specific torrent that contained information about *108 files*. The EPA IP address did not obtain downloads or images by simply associating with the torrent. Associating with the torrent only provided the EPA IP address with names of files, or a catalog. Moreover, the torrent the EPA IP address associated with contained information regarding *108 individual files*, not all of which were illegal child pornography. Detective Wistocki could not know what term the EPA IP address entered that led it to that torrent, what file described within the torrent the EPA IP address wanted, or even if the EPA IP address ever searched for, downloaded, or attempted to download any of the 108 files. Regardless of whether some of the file names within the torrent matched names of files on the ICAC COPS database, such a match would not allow Detective Wistocki to confirm that the EPA IP address downloaded child pornography, let alone a single file described by the torrent. Again, accessing the torrent and obtaining the names of files does not mean any download has taken place, or is in the process of taking place, or will ever take place. Moreover, detective Wistocki specifically knew that the EPA IP did not download or have any of the files, or parts of files, containing child pornography on any of the EPA computer.

Contrary to what he actually observed, Detective Wistocki made it seem as if the EPA IP address was downloading images and had obtained images in the past. In fact, Detective Wistocki went so far as describing four files that the EPA IP address purportedly downloaded, and when it downloaded the files. S.W. Aff. 13-15. In reality, Detective Wistocki never observed a single file downloaded by the EPA IP address. The time stamps Detective Wistocki listed refer to when the

Torrential Downpour discovered that the EPA IP address was associated with the torrent, identified by its info hash value, not when the EPA IP address downloaded a file. (see Exhibits 2, 3, and 4)

Finally, Detective Wistocki retold the same lies when detailing what he purportedly observed while investigating Mr. O'Hara's IP address. Specifically, Detective Wistocki asserts that he determined that Mr. O'Hara's IP address "downloaded hundreds of files of child pornography." S.W. Aff. 18. Detective Wistocki reached this conclusion because the "infohashes sought by [Mr. O'Hara's IP address] were identical to the infohashes downloaded through the EPA IP address, meaning they had the same series of photos or videos, most of which were child pornography." *Id.* As described above, downloading an info hash values, *i.e.* a torrent, does not mean that a user has downloaded a single file. What Detective Wistocki actually discovered was that Mr. O'Hara's IP address associated with the same torrent as the EPA IP address, and therefore had the same names of files not "the same series of photos or videos."

C. The Affiant Deliberately Made the False Statements

An affiant acts with reckless disregard when he "in fact entertain[s] serious doubts as to the truth of his allegations." *United Sates v. Lowe*, 516 F.3d 580, 584 (7th Cir. 2008). Though this standard requires more than mere negligence, it "may be proved from circumstances showing obvious reasons for the affiant to doubt the truth of the allegations." *Williams*, 718 F.3d at 650. This is not a case of oversight, or negligence. The Affidavit asserted that Detective Wistocki observed things that he did not. Detective Wistocki never observed downloads, and never compared files he saw on the EPA IP address with known child pornography files. Detective Wistocki knew he did not do these things, yet said he did anyway. In fact, the affiant's assertion that detective Wistocki observed EPA IP to be downloading hundreds of files containing child pornography, totally contradicts detective Wistocki's assertion just a few sentenced away where

he declares "there was no direct download from this IP address to my computer." He deliberately misrepresented his investigation.

Even more disturbing was the false assertion that "the device at [EPA IP] was the sole candidate for each download. The Affiant and detective Wistocki both knew that such a statement is a complete fabrication. They knew that neither the computer associated with EPA IP nor O'Hara's IP had any actual contraband files and no "downloads" were ever made. Any argument to the contrary would require 'alternative facts' not present here. Moreover, all the false claims detailed above were not a mistake, but rather a complete disregard for the truth. Before seeking the search warrant at issue here, Detective Wistocki authored two search warrant affidavits asking a state court judge in Will county to issue search warrants for Mr. O'Hara's home and work. (Exhibit 5 and 6). Detective Wistocki used the same false assertions in the affidavits he authored as were used in the affidavit in question. There can be no questions that Affiant and Detective Wistocki made material false statements in the affidavit.

D. Judge Finnegan Would Not Have Found Probable Cause if the Affidavit Did Not Include These False Statements

If accurate information replaced Detective Wistocki's lies, Judge Finnegan would not have found probable cause. An affidavit sets forth probable cause when "the issuing judge can make a practical, common-sense determination that there is a fair probability that contraband or evidence of a crime will be found in a particular place." *United States v. Mullins*, 803 F.3d 858, 861 (7th Cir. 2015). Though the information provided in the affidavit need not rise to proof beyond a reasonable doubt, it "must provide the magistrate with a substantial basis for determining the existence of probable cause." *Illinois v. Gates*, 462 U.S. 213, 239 (1983).

In this case, the info hash values Detective Wistocki observed referenced a torrent that contained information about 108 files. As detailed above, this does not mean that either IP address

cited downloaded a single one of those 108 files. All associating with a torrent provides a user is the files' names and other descriptive information that is not contraband. Simply accessing a torrent sheds no light as whether the user has downloaded, or is downloading any one of those files. Assessing any torrent is not illegal, and certainly does not rise to the level of probable cause to believe a person has downloaded contraband. Had the Affidavit stated that law enforcement only discovered that the EPA IP address had a torrent database file, and Mr. O'Hara's IP address had the same database, containing many info hash values which were not even associated with child pornography, Judge Finnegan would not have had probable cause to believe that actual downloaded child pornography files would be found on the computers.

CONCLUSION

At this stage, Mr. O'Hara is required to only make a preliminary showing that the Affidavit deliberately supplied false statements, and that Judge Finnegan would not have found probable cause without those false statements. *Franks*, 438 U.S. at 171. Mr. O'Hara has met this initial burden, and this Court should grant his request to conduct an evidentiary hearing. There, Mr. O'Hara will demonstrate by a preponderance of the evidence the same above outlined elements, and ask this Court to suppress the search warrant and all evidence obtained in connection with the execution of this illegal search warrant.

Respectfully submitted,

_____

Gal Pissetzky
Attorney for Mr. O'Hara
53 W. Jackson Blvd., Suite 1515
Chicago, IL 60604
(312)566-9900

CERTIFICATE OF SERVICE

The undersigned, Gal Pissetzky, hereby certifies that in accordance with Fed.R.Crim.P. 49, Fed.R.Civ.P. 5, and the General Order on Electronic Case Filing (ECF), the

MOTION FOR SUBSTITUTION OF ATTORNEYS

was served on November 20, 2017, pursuant to the district court's ECF filers to the following:

Assistant United States Attorney's Office
219 S. Dearborn St., 5th Floor
Chicago, IL 60604

Respectfully submitted,

/s/ Gal Pissetzky
Gal Pissetzky
Attorney for Mr. O'Hara
53 W. Jackson Blvd., Suite 1515
Chicago, IL 60604
(312)566-9900